This article was originally published by Law360 on September 12, 2019.

Audit Shows Where DOD Cyber Enforcement Is Headed Next

By **Todd Overman and Roee Talmor**

The U.S. Department of Defense inspector general issued a report on July 23 summarizing the findings of an audit into the protection of controlled unclassified information, or CUI, on contractor networks.

Based on an in-depth review into nine contractors, the audit uncovered some common practices that fall short of meeting the standards set forth in National Institute of Standards and Technology Special Publication 800-171, which contractors are obligated to follow under Defense Federal Acquisition Regulation Supplement 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Todd Overman

Roee Talmor

To address these exposed deficiencies, the report recommends that the DOD develop a plan to better verify and enforce compliance with NIST standards, including remedial action against noncompliant contractors. The DOD, in response, has already agreed to implement many of the listed recommendations.

The report is a sign of things to come and should serve as guidance to contractors to ensure that they are meeting the requirements of DFARS 252.204-7012.

Background

CUI is a designation for unclassified information that requires proper safeguarding from malicious actors. Compromise of such information poses risks for national security that are far more than theoretical.

According to the report, private enterprises constitute particularly likely targets for cyberattacks. Indeed, cyber-theft has cost American industries more than $600 billion. Private actors' failure to safeguard information puts DOD investments at risk and may expose operational capabilities or defense system specifications to attacks from hostile actors.

To ensure adequate safeguarding of information, DFRAS 252.204-7012 requires contractors who maintain DOD information on their networks to implement the security standards set forth in NIST SP 800-171.

These standards include implementing user authentication, control of user access, media protection, management of vulnerabilities and rapid response to security incidents.

DOD Instruction 5010.40 requires departmental components to implement a comprehensive system of internal controls to ensure that programs are operating as planned.

The objective of the inspector general’s audit was to determine contractor compliance with security control and assess the sufficiency of DOD oversight. The results revealed significant gaps in compliance, both by the DOD and individual contractors.

Shortcomings Discovered in DOD Audit

The audit exposed deficiencies as to each of the examined contractors. Nearly all the companies did not always mitigate vulnerabilities on their networks and systems.

More specifically, two did not scan their network for vulnerabilities and six did not mitigate high vulnerabilities within the timeframes identified in the contractor’s management programs.

Also common were the inconsistent use of multifactor authentication and failure to require sufficiently lengthy and complex passwords — seven contractors fell short of satisfying these standards.

Over half of audited contractors failed to restrict the number of individuals able to store information on removable media devices, such as a USB hard-drive, or limit data transfer to nonencrypted devices.

Likewise, a little over half of the contractors imposed system lockout after inactivity or unsuccessful logon attempts that are sufficient to prevent unauthorized access.

Less common deficiencies included:

- Overallowance of system access based on a user’s assigned duties.
- Failure to document and track cybersecurity incidents.
- Lax oversight of third-party network service provides.
- Failure to consistently generate and review system activity reports.

Moreover, the audit revealed that the DOD component contracting offices did not develop or implement sufficient oversight processes to ensure contractor compliance with NIST-required security controls.

Various component contracting offices expressed confusion over whether they possess authority under existing contractual language to oversee contractor compliance with NIST security requirements. This confusion, according to the report, can be traced to the absence of explicit language in DOD contracts that enables the various contracting offices to conduct on-site compliance assessments.

Even more fundamentally, many component contracting offices did not track which contractors maintained CUI on their networks, rendering meaningful oversight nearly impossible.

Recommendations in Response to DOD Audit

To address the deficiencies in contractor compliance and DOD oversight, the report contains a number of specific recommendations that, if implemented, will significantly strengthen enforcement of NIST standards. The report recommends that the DOD fundamentally overhaul its oversight and enforcement procedures, beginning at the request for proposals and source selection stage.

Specifically, the report recommends that the principal director for defense pricing and contracting, or DPC, require contractor compliance with NIST requirements prior to awarding the contract.

The recommendations further encompass an annual compliance check throughout the performance period. The DPC, according to the report, should likewise introduce policies that require DOD component contracting offices to keep an accurate accounting of contractors who maintain, or have access to, CUI during contract performance.

Perhaps most importantly from the contractor's perspective, the report recommends that the various components take corrective action against contractors noncompliant with NIST standards. The report likewise recommends that the various DOD components develop and implement a plan to verify that contractors identify and correct the contractor-specific deficiencies identified above.

Likely Increase in Oversight Efforts

In response, the acting director of DPC agreed with the need to take corrective action against noncompliant contractors. He further indicated that the DPC will undertake a pilot program to develop a department wide approach for assessing contractor compliance with NIST SP 800-171 requirements.

The planned pilot program is consistent with the unmistakable trend toward a more robust cybersecurity enforcement regime. For example, the DOD recently announced it plans to develop a new certification framework called "Cybersecurity Maturity Model Certification." The planned framework, released for public comment on Sept. 4 and scheduled to be rolled out in 2020, will require a contractor's network be certified compliant by an accredited third party auditor prior to contract award.

How the planned pilot program will interact with the DOD's announced plans for the cybersecurity maturity model certification and the shift to third party certifiers is an open question but should serve as another signal that the DOD is ramping up its oversight and enforcement efforts. Indeed, contractors who fail to comply with NIST standards may soon find themselves at a significant competitive disadvantage.

Todd R. Overman is a member and Roee Talmor is an associate at Bass Berry & Sims PLC.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.